Statement to

DEPARTMENT OF HEALTH AND HUMAN SERVICES

NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

SUBCOMMITTEE ON HEALTH DATA NEEDS, STANDARDS, AND SECURITY

Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)
A Perspective from Early Implementers of the HIPAA Security Aspect of Administrative Simplification

July 14, 2000

By: Jonathan S. Zimmerman
General Manager of
Healthcare Data Exchange Corporation (HDX) and
Senior Manager of HIPAA Initiatives
Shared Medical Systems Corporation (SMS)
Subsidiaries of Siemens Corporation

Mr. Chairman and members of the committee, I am Jon Zimmerman, the General Manager of HDX, and the Senior Manager of HIPAA Initiatives for Shared Medical Systems (SMS), both wholly owned subsidiaries of Siemens Corporation. On behalf of HDX and SMS, I want to thank you for the opportunity to testify today as an early implementer of Administrative Simplification.

In the interest of brevity and your time, I would like to include by reference the descriptions of HDX and SMS as presented yesterday by my colleague, Don Bechtel. To the best of my knowledge, nothing of significance has changed between yesterday and today.

What I will add is that in the last year or so, I have directly spoken to or engaged in over 100 various provider, payer or industry forums or discussions. Many of these are working directly with a health systems' senior management team to kick-off their HIPAA preparation initiatives. Thus, I am bringing a significant amount of listening and collective practical experience in my remarks to you today.

What I will attempt today is to shed some light, based on our team's experience, on how we, as an industry, can cope with HIPAA's mandates in an economically challenged,

highly fragmented, complex, technologically and culturally diverse environment. To do so, I will try to put my remarks in context of our view of HIPAA, identify how this relates to the Health industry; describe why it is important to fit with other relevant business and industrial environmental factors; provide some examples of progressive and valuable initiatives currently underway; provide a few observations and recommendations; then tie it all back together.

Administrative Simplification – Security

Description

I know this committee is very familiar with HIPAA and its Administrative Simplification components, but to set my remarks in context, I would like to very briefly review HIPAA's Administrative Simplification construct and specifically, Security.

First, I am hopeful and confident that we will be proven right in our support of the validity and construct of this legislation and attendant regulations. The fundamental approach of "adopting standards" has visionary aspects in its broad and long-term implications. To us, adopt means "use what works"; do not create where you do not have to. Standards implies "what has been agreed to" in either a formal or informal (de facto) consensus process. HIPAA needs to stand the tests of time in an era of unprecedented rapid technological change.

When HIPAA was in its formative stages, the commercial and consumer use of the Internet was essentially non-existent. Today, the Internet has profoundly and irreversibly affected our economy, our culture and how information, knowledge and commerce are exchanged across the globe. Even with such a monumental change, HIPAA is extremely relevant, applicable and perhaps, essential to the industry. My compliments to the visionaries who engineered legislation that is already proving it can stand the tests of time and rapid change.

HIPAA's five "security tracks" upon which I will base my remarks are:

- Administrative Procedures – How one defines, communicates, administers and monitors acceptable practices to protect the confidentiality of patient information and business operations.
- Physical Safeguards – How the information is physically protected from disclosure or harm (destruction or damage).

- Technical Security Services – How access to the information is enabled only for those who need to know within the context of their responsibilities at a given point in time.
- Technical Security Mechanisms – How the information is properly protected during transmission and storage.
- Electronic Signature – How to ensure that those who use Electronic Signatures as part of their business processes can be irrefutably, uniquely and specifically identified.

Affected Parties

When one considers the scope and access to "individually identifiable health information" it is difficult to imagine how anyone is not affected by HIPAA Security. Payers, Providers and Health Information Clearinghouses, plus their trading and business partners encompass a wide spectrum of American Industry. Most of us have had some sort of proactive or reactive health care in the last two years. Most of us have a doctor or a health care facility where we can receive care in a relatively short period of time. Most of these facilities have some sort of electronic processing for billing or other administrative functions. Many of these business are somehow electronically interconnected, and getting more so everyday. These connections carry individually identifiable health information and each of the systems, for some period of time, store and maintain these data for the purposes of delivering care or reimbursement for care delivered.

Thus, the scope and complexity of securing information in this vast and dynamic environment is both daunting and imperative. Measured steps toward well-defined desired outcomes that allow the industry to leverage its existing practices and infrastructure are a critical component of our future security. Further, we must be prepared to blend our industry's efforts with those of the rest of American or international commerce so we can quickly and confidently take advantage of proven advancements and economies of scale.

HIPAA's Own Dynamic Tension

Like many great works of art, HIPAA possesses within itself a constant dynamic tension, two forces pulling against one another, eternally struggling for balance. These forces are those of efficiency and security. The nature of our health care delivery and payment system demands that many parties be involved with each episode of care. Each episode

of care carries with it certain amounts of information. The more complex or unusual the case, the more data must be managed. Easy, open access to anyone who needs to see or use the data would logically be the best path to new efficiencies. Interconnected networks of computers of any impacted parties would help improve access and efficiency while reducing cost.

This is a recipe for a privacy disaster. Information security, by its very nature, is intended to restrict access to the fewest number of possible parties. So, how can one improve efficiency by providing efficient access while improving security practices to protect individual's rights and business operations? That is precisely why I'm here, no one has figured it out….yet.

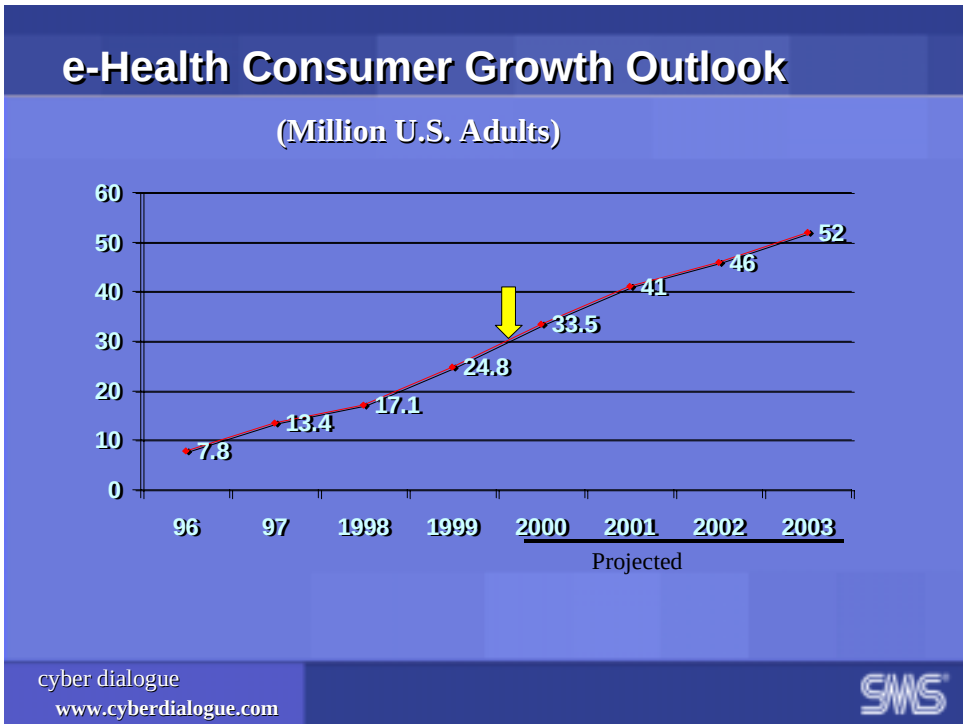
Relationship to the Health Industry

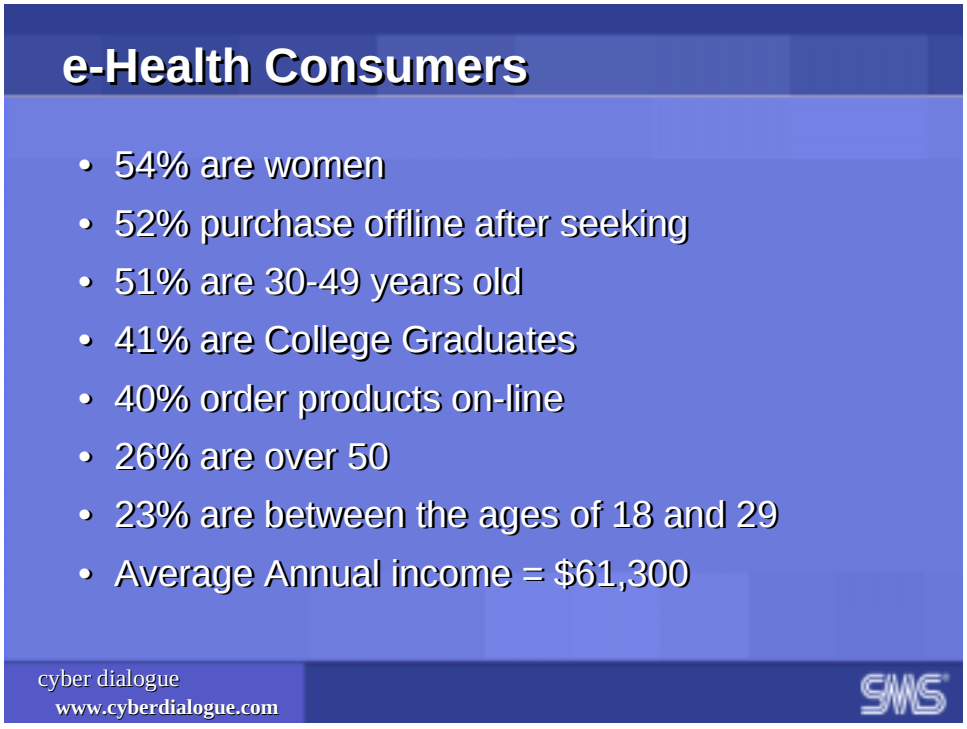
Base of Security Practices

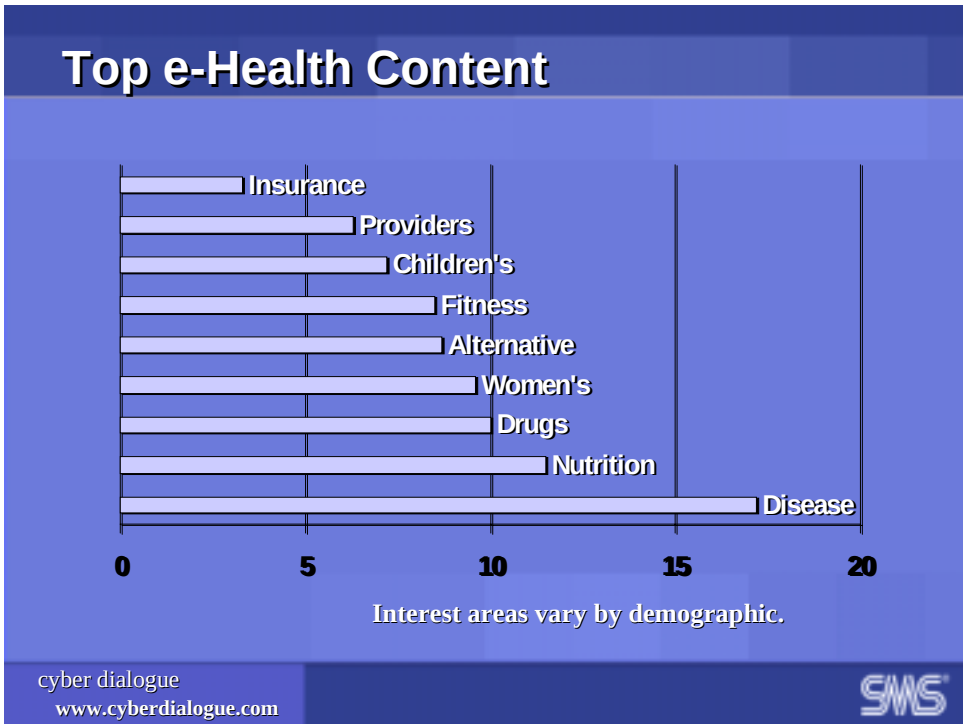
Part of the good fortune we have is an environment where people inherently care about how they do their work and how they protect their patients. To that end, protecting privacy via good security practices is somewhat institutionalized and ingrained in our culture already. Many of our payer and provider customers have solid security policies, procedures and practices in operation today. Certifying and monitoring them against defined and measurable standards is where much work lies ahead of us.

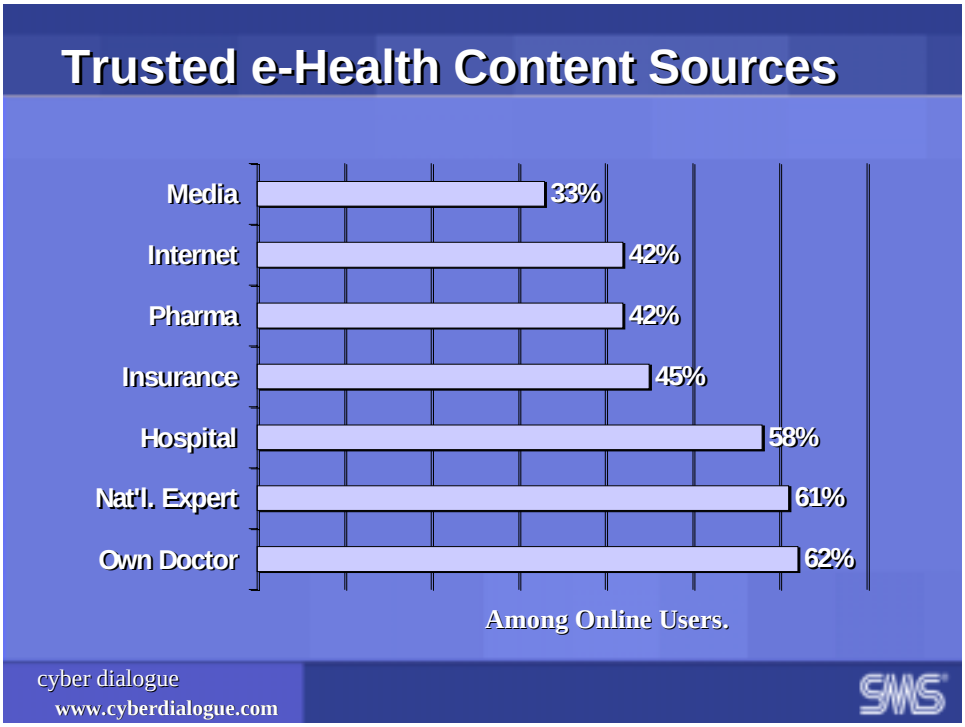
We have a head start, but a long race to run. Why? Because so many health businesses are reaching further out beyond their current systems and networks to use attract new customers or reduce operational costs. Thus, we have a moving and expanding target. Targets that will effect profound changes in the operations of the businesses that make up this industry.

To illustrate these points, I have included the following charts that contain data from studies by CyberDialogue, an Internet Consumer/Business Behavior Research firm:


e-Health Consumer Growth Outlook
(Million U.S. Adults)
60
50
40
30
20
10
0
7.8
13.4
17.1
24.8
33.5
41
46
52
96
97
1998
1999
2000
2001
2002
2003
Projected
cyber dialogue
www.cyberdialogue.com
SMS


e-Health Consumers
• 54% are women
• 52% purchase offline after seeking
• 51% are 30-49 years old
• 41% are College Graduates
• 40% order products on-line
• 26% are over 50
• 23% are between the ages of 18 and 29
• Average Annual income = $61,300
cyber dialogue
www.cyberdialogue.com
SMS


Top e-Health Content
Insurance
Providers
Children's
Fitness
Alternative
Women's
Drugs
Nutrition
Disease
0
5
10
15
20
Interest areas vary by demographic.
cyber dialogue
www.cyberdialogue.com
SMS


Trusted e-Health Content Sources
Media
33%
Internet
42%
Pharma
42%
Insurance
45%
Hospital
58%
Nat'l. Expert
61%
Own Doctor
62%
Among Online Users.
cyber dialogue
www.cyberdialogue.com
SMS

Significant Concerns

The most significant areas of concern are in how to change or enhance secure operations and the economic impact of doing so. Changes require investments. Positive and progressive change require solid understanding of one's current state of affairs, clear depiction of goals, and a solid set of inter-related steps forward. All of these take time and cost money to do well.

These changes fall upon the provider industry just as we are under some of the most severe economic constraints in history. Hospitals are running at their lowest margins in recent memory and more are in the red than ever before. Couple this with the impending affects of OPPS where top line revenue will be reduced with no attendant reduction in costs, thus creating more pressure. Of course, this follows a unique year where much of information technology investments went toward just staying in place (Y2K preparation) as opposed to making investments to improve efficiency. So, we are now reaching the triple witching hour of thin or non-existent margins, declining reimbursements and increased demand for Security investments to satisfy pending regulations. Thus, every drop of leverage or economic value we can squeeze out of HIPAA investments is vital to the overall success of the industry.

Relationship to Our Current Business Environment

Fortunately, the health industry is not alone. E-business has invigorated our economy and exciting new innovations are boiling all around us. Moore's law of computing where costs will drop 20% per year and speed will double every 18 months is still in effect. Interconnecting business processes of suppliers, customers, partners and consumers through standards-based computer networks is driving innovation and attracting investment across this country and the world.

What does this mean to us? As other industries solve problems and create new efficiencies, by adopting their standards, health care can reap the same rewards. Just look at the last two cover stories from InformationWeek. On July 3rd, they cover the Federal Legislation raising the validity of Electronic Signatures to the legal status of paper-based signatures. This could relieve our industry of the burden of coming up with our own standard to develop, maintain and enhance.

Now look at July 10th, there is a recognized gap between what companies have in place for computer security and what they know they need. This breeds opportunity and attracts investment. Yet another chance to leverage other's success for our own.

Finally, consider the impact and rapid proliferation of cell phones, the Palm Pilot and other handheld devices in the last 18 months. We are clearly extending from our base as a mobile society to a mobile work force to mobile work that demands mobile data. Healthcare is no different and we are compelled to learn better and faster about how to capitalize by adopting technologies and standards from any industry that makes sense.

With so much of our national corporate information assets travelling around on wires and through the cellular networks today, it is easy to see why Information Security and Privacy are emerging as national business priorities. This is evidenced by the news broadcasts on Wednesday of this week. At least two national news programs (I can only reference two because I can only watch two at a time) featured privacy and security as featured stories. Fortunately, there are some encouraging examples of leaders in our taking charge and moving forward today.

Examples of Promising Work Underway

National Activities

On both a national and regional basis, there are a number of inter-related initiatives underway. I will mention some of them, but by no means does my lack of inclusion of any particular initiative indicate a lack of respect or value for the works in progress.

A few that come to mind are:

CPRI Toolkit

This work is proving to be one of the definitive efforts on how to gather and document best practices as it relates to protecting computer-based patient records. Drs. Ted Cooper from Kaiser Permanante and Jeff Collman from Georgetown continue to lead the effort to attract examples of how people can protect, store, transmit and manage patient information safely and securely.

Security Summit

This initiative was created as a result of one of the early industry broadcasts about what HIPAA Security was all about and how the industry should begin to prepare. John Pamigiani (at the time from HCFA) Barbara Clark, Bill Schooler and Pat Kunzee (HCFA), led a discussion to over 1,000 conference call attendees. As a result of the call, and at the suggestion and leadership of Johns Hopkins Medicine, WEDI and SMS put out a call to the industry to work together to begin to develop implementation guidelines that

are scalable, reasonable and implementable regardless of the size and complexity of the business.

Some key associations, like MGMA and ADA, who brought a critical and valuable perspective to the effort, supported this group. In all 173 participants from payers to providers to consultants to lawyers to technology, applications and services vendors came together to draft a document specifically to assist in providing the answer to a burning HIPAA Security question: How do I know if I'm doing it right? Without HCFA's support, encouragement, guidance and participation, the Security Summit would not have had nearly the impact that it has thus far. To them, once again, we all say "Thanks."

The Security Summit and the CPRI toolkit initiatives continue to work collaboratively and we hope to generate complementary deliverables in support of HIPAA Security.

AFECHT/WEDI Interoperability Pilot

WEDI and AFEHCT also joined forces to work through a painstaking and illuminating process to define and document the issues associated with Interoperability. Choice is inherent in our culture and our industry loves to make and defend their choices. While this has been valuable, too much of a good thing can hurt. There are many competing schemas and approaches for security, but to enable exchanging information, the solutions must not only work within themselves, they must cooperate and inter-operate with others. Much easier said than done, and with each State allowed setting its own "Security Ceiling" this issue is far from going away. Many valuable lessons were learned from these initiatives. These are well documented at the AFEHCT and WEDI web-sites.

Strategic National Implementation Process - S.N.I.P.

The latest and perhaps most vital undertaking to date is SNIP. On this panel, we have two of the driving forces behind SNIP, Chris Stahlecker and Larry Watkins. I will not take the committee's time to describe their initiative. However, I would be remiss if I did not make mention of the important undertaking they are in the process of launching.

Regional Activities

As we all know, while Healthcare is of national concern, it remains a local or regional issue. Payers, providers, patients and consumers all live and work within a community structure that falls under state, federal and local jurisdiction and customs. Thus, we do

not expect a "HIPAA Big Bang" rather we expect to see HIPAA adopted in varying stages to varying degrees at varying rates in different geographic settings. All of them share the characteristics of having providers, payers and other members of their locale working in a structured manner to help the entire community prepare for and embrace HIPAA. Some of the most prominent initiatives are listed below. I encourage us all to continue to monitor their activities and progress over the comings months. I am very confident that many valuable lessons will be gained from each of them. Below is a short list of just three regional groups with whom I have interacted and have personal knowledge. For convenience, I have them listed with their website addresses and a key distinguishing feature or two for each.

NCHICA - http://www.nchica.org/

North Carolina Health Information and Communications Alliance.

Early Start, Great Structure, Effective Security Assessment Tool

GDAHC – HIAG – MHMIS - http://www.hiag.org/hiag

Greater Detroit Area Health Council – Health Information Action Group – Michigan Health Management Information Systems

Solid Start, Employer Participation, Uses Automotive Network Exchange Extranet from the GM, Ford and DaimlerChrysler.

MHDC - http://www.mahealthdata.org/

Massachusetts Health Data Consortium Inc.

Very Comprehensive, Very Active, Collaborative Model, De-identified Data

I am aware of quite a few more regional activities in places like Minnesota, Utah and others. The good news here is that these folks are off and running in their compliance initiatives, recognizing the complexity and that this will take careful study and time. The other good news is that they all demonstrate the fact that it is virtually useless to be compliant with HIPAA by oneself, you must involve your partners. *(It is sort of like playing tag while alone, I suppose it is theoretically possible, there can be a lot of activity, but not much is actually accomplished.)* The challenge is that each community will probably address issues in a slightly different way, creating nuances and potentially diluting the value of standards and prolonging a national rollout. We should find a

forum to discuss how to monitor these situations and work to avoid duplicative and conflicting efforts.

Recommendations

This brings me to the recommendations we would like to offer to the panel today. The five we have selected are:

Stretch the Limits – Take the Bumps

With any progressive effort, people must extend beyond the status quo. You are hearing about a lot of volunteer efforts of people devoting themselves beyond their jobs to help the industry. I encourage the members of the government agencies to continue to take prudent risk and follow their conscience, as they need to, at times, stretch beyond the limits of their authority. Early warnings and good hints to the Industry are most welcome and constructive.

Also, know that we will not execute with perfection. Allow us to make good faith errors, gently point out suggested improvements, but do not punish the well intended. For malicious violators, hit the hard, but for those who slip, please be prepared to assist, not vilify.

Sanction and Promote Cooperative Processes

Get and stay in the game with us. I have seen some welcome assistance from the Government in a number of situations. Please keep it coming. It gives us energy, validation and helps ensure we stay on the right course. The Industry only wants to make these kinds of investments once. So, as much as you can, stay with us and help.

When you like what is going on, tell someone. In fact, I have seen Karen Truedel (HCFA) do this very well on a couple of occasions. This is precisely what is needed to provide the necessary assurance and stimulation to drive positive momentum.

Clarify Goals, Objectives and Expectations

Nothing drives inertia like uncertainty. This is one of the biggest challenges we face. A lack of clarity begets both argument and debilitating confusion. The more that the Government can provide precise or illuminating descriptions of the “desired outcomes”

the more accurately the Industry can target our efforts. Shooting in the dark is a bad thing; we might hit something or someone we like.

As our objectives become clearer, measurable descriptions of "bands of tolerable behavior" would be very helpful. The adage "you can't manage what you can't measure" is very applicable here. We require some ability to know how and what to measure so we can gauge our success in compliance.

Actively Support Examples

Nothing is more illuminating and valuable in implementing complex systems than clear examples. The transactions have implementation guides because they are needed. The number of variables is too great to make the standards useful unless applied to situations we can understand, digest and replicate. In this context, Security is no different and we urge you to continue and accelerate your work with Industry in supporting valid "how-to" and "what-if" guidance.

Economically Stimulate Technology, Industry and Government Collaboration

This is an industry under severe pressure, however you look at it. Some for good reason, some not. Consider ways to reward or provide incentives for achieving HIPAA compliance. Often we refer to the carrot and the stick. We need to spend more time on the carrots; enough people are focused on the stick. Two mechanisms the Government has used in the past might well work in this situation. Please consider providing enhanced reimbursement structures or tax relief for demonstrated HIPAA compliance.

We know that one of the stimulants or rewards of national HIPAA compliance is a more cost efficient health system. These improvements will yield benefits for patients, providers, and payers. Since the federal and state governments carry so much of the fiscal burden of health care, it stands to reason that seeding initiatives now will accelerate the Government's ability to realize savings and relieve some of the pressure. So, let's find a way to put our money where our mouth is and make the progress toward efficiency and security demonstrated so well by so many other industries.

Summary

In conclusion, we firmly believe that we are doing the "right thing". This, in itself, drives momentum through difficult or confusing situations. We must maintain a focus on our objectives and, regardless or parochial wrangling, stay the course. We must all be as clear and precise as we possibly can. That will keep allow us to establish and maintain traction

with minimal distraction and resistance. Timing and delivery against promised dates is critical. Delays destroy momentum. Please let us help you avoid them. We should all not be overly concerned about stretching beyond our perceived limits to achieve a defined objective. As with anything new, we will make mistakes. Let us, but help us get back on course quickly. Punishment is not always the best stimulant to action, sometimes economic incentives work well too. Fostering cross- pollination of ideas and progress across geographies will help propel us towards the goals we collectively establish.

Finally, listening patiently to other perspectives is crucial. While addressing every potential situation or concern is not practical, listening has brought much light and fostered tremendous progress. That's why this forum is so valuable and has proven to be a helpful instrument of progress.

Mr. Chairman and members of the committee, this concludes my statement. Thank you.